GIBSON DUNN

August 27, 2015

THE THIRD CIRCUIT UPHOLDS THE U.S. FEDERAL TRADE COMMISSION'S AUTHORITY TO REGULATE CYBERSECURITY

To Our Clients and Friends:

The Federal Trade Commission's longstanding effort to establish itself as the primary federal regulator of cybersecurity survived its first appellate test on Monday when the Third Circuit allowed the FTC to continue pursuing its case against Wyndham Worldwide Corp.[1] The FTC sued Wyndham after the hotelier suffered three data breaches that allegedly compromised the payment card information of more than 600,000 customers. The FTC alleged, among other things, that Wyndham's failure to use encryption, firewalls, and non-obvious passwords constituted an "unfair" practice under Section 5 of the FTC Act. The district court denied Wyndham's motion to dismiss the FTC's case, but allowed Wyndham to pursue an interlocutory appeal. A unanimous Third Circuit panel affirmed the district court's ruling in an opinion the FTC touted as a "must read for business executives and attorneys."[2]

The History of the FTC's Cybersecurity Enforcement Program

Section 5 of the FTC Act dates to 1914 and states that "unfair or deceptive acts or practices in or affecting commerce, are . . . unlawful."[3] As one would expect from a statute that dates to World War I, there is no mention of cybersecurity. However, the FTC has long taken the position that Congress intended "unfair" practices to be defined broadly and flexibly to allow the agency to effectively protect consumers as the economy and technology develop.[4]

The FTC first asserted that its authority under Section 5 encompassed investigating and prosecuting companies for insufficient data security procedures in 2002.[5] During the course of the next ten years, the Commission pursued more than 35 enforcement actions alleging inadequate and/or overstated cybersecurity practices. Each of these actions resulted in a negotiated consent agreement, and no target elected to test the agency's allegations or statutory authority to regulate cybersecurity. That changed when the FTC sued Wyndham in June 2012.

The pending litigation with Wyndham has done little to chill the FTC's enthusiasm for bringing cybersecurity enforcement actions. Rather, the agency has continued to bring enforcement actions at an increasing rate and issued a public statement in January 2014 "marking" its 50th data security enforcement action.[6] One of the FTC's post-Wyndham targets, LabMD, a clinical testing laboratory based in Georgia, has also elected to litigate the agency's authority to regulate cybersecurity. That dispute is pending in the FTC's administrative court and could lead to a second appellate decision addressing the FTC's jurisdiction to regulate cybersecurity practices.[7]

The FTC's efforts to regulate cybersecurity extend beyond enforcement actions. The agency has devoted a portion of its website to data security and has issued policy statements and guidance for business. The Commission recently summarized its approach to data security as hinging on "reasonableness: [specifically,] a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities."[8]

The Third Circuit's *Wyndham* Decision

Factual and Procedural Background

In June 2012, the FTC sued, alleging that hackers had obtained unauthorized access to Wyndham's computer networks on three separate occasions between 2008 and 2010, leading to its customers facing more than $10.6 million in fraudulent payment card charges. The FTC claimed that Wyndham violated the unfairness prong of Section 5 by "fail[ing] to employ reasonable and appropriate measures to protect personal information against unauthorized access."[9] Specifically, the complaint alleged that Wyndham:

- Allowed its hotels to store payment card information in clear readable text;
- Permitted employees to use easy-to-guess passwords to access its property management systems;
- Failed to use firewalls and other "adequate information security policies and procedures";
- Inadequately restricted third-party vendors' access to its network and servers;
- Failed to take "reasonable measures to detect and prevent unauthorized access" to its computer network; and
- Did not follow "proper incident response procedures," allowing hackers to use similar methods in each attack.[10]

The FTC also alleged that Wyndham's 2008 privacy policy was deceptive (Section 5 of the FTC Act separately bars both "unfair" and "deceptive" practices), because the privacy policy overstated the company's cybersecurity. Although the deception claim was not before the Third Circuit on appeal, the FTC's allegations concerning Wyndham's privacy policy played a role in the court's decision, as explained below. Wyndham moved to dismiss both the unfair practice and deceptive practice claims, and challenged the FTC's authority to regulate data security.[11]

The district court denied Wyndham's motion, but certified its decision on the unfairness prong of Section 5 for interlocutory appeal, and the Third Circuit granted Wyndham's application for appeal.[12] Writing for a unanimous three-judge panel, Circuit Judge Ambro affirmed the district court's decision.[13]

Section 5's Bar on "Unfair" Practices Authorizes the FTC to Regulate Cybersecurity

Wyndham attacked the FTC's jurisdiction and allegations from multiple angles. First, Wyndham argued the FTC's allegations were statutorily insufficient. Wyndham did not question that the FTC's claims met the requirements specified in Section 15(n) of the FTC Act, which requires an "unfair" practice be (1) likely to cause "substantial injury"; (2) unavoidable by "consumers themselves"; and (3) not be "outweighed by countervailing benefits to consumers or to competition."[14] Instead, Wyndham asserted that the FTC's allegations failed to meet additional requirements implicit in the FTC Act. Specifically, Wyndham asserted that the FTC must show that the conduct at issue is "unscrupulous or unethical."[15] The Third Circuit held that the Supreme Court rejected this argument in *F.T.C. v. Sperry & Hutchinson Co.*, 405 U.S. 233, 244 n.5 (1972).[16] Wyndham further asserted that the "plain meaning" of "unfair" implies a requirement that the FTC demonstrate that the challenged conduct is "not equitable" or involves "injustice, partiality, or deception."[17] The Third Circuit brushed this argument aside, stating that even if such a requirement exists, a "company does not act equitably when it . . . exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business."[18]

Second, Wyndham argued that when a business itself is victimized by criminals, it "does not treat its customers in an 'unfair' manner."[19] Rejecting this argument, the court explained that the FTC Act "expressly contemplates the possibility that conduct can be unfair before actual injury occurs."[20] More important for the Third Circuit was that Wyndham's argument runs contrary to fundamental tort law principles: "that a company's conduct was not *the most* proximate cause of an injury generally does not immunize liability from foreseeable harms."[21] As such, that Wyndham, like its customers, was a victim of a criminal act did not immunize Wyndham from liability.

Third, Wyndham argued that Congress's enactment of various laws that touch on the FTC's role in regulating cybersecurity--including a recent amendment to the Fair Credit Report Act (directing the FTC and other agencies to develop regulations for the proper disposal of consumer data), the Gramm-Leach-Bliley Act, and the Children's Online Privacy Protection Act--show that Congress does not intend the FTC to have broad regulatory authority over corporate cybersecurity practices under the FTC Act.[22] The court disagreed, and suggested that the recent laws were meant to work in concert with the FTC Act to govern company cybersecurity practices. The court noted that each of the laws specifically requires the FTC to issue implementing regulations. The court found no significance in the fact that the FTC had, in the past, attempted to obtain from Congress certain authority to regulate cybersecurity practices. Instead, the court viewed these as the FTC's efforts to *broaden* what the FTC viewed as its already existing authority.[23]

Wyndham Received Fair Notice

Wyndham also challenged the complaint on the basis that it did not have fair notice under the Constitution's Due Process clause that its specific cybersecurity practices could fall short of the requirements of the unfairness prong of Section 5. The Third Circuit held that notice is constitutionally sufficient "as long as the company can reasonably foresee that a court could construe its conduct as falling within the meaning of the statute."[24]

Wyndham's lack-of-notice argument, according to the court, fell "well short" given the allegations in the complaint--i.e., it wasn't that the complaint alleged that Wyndham had *weak* cybersecurity protocols in place, rather, in many instances, the complaint alleged that Wyndham had *none at all*. Additionally, the court was particularly dismissive of this argument because Wyndham "was hacked not one or two, but three, times . . . certainly after the second time Wyndham was hacked, it was on notice of the possibility that a court *could* find that its practices fail the cost-benefit analysis."[25]

Finally, the court pointed to several FTC publications and administrative enforcement actions that placed Wyndham on notice that its conduct could be construed to be proscribed by the FTC Act. Specifically, the court pointed to a 2007 FTC guidebook entitled *Protecting Personal Information: A Guide for Business*, which "describes a 'checklist[ ]' of practices that form a 'sound data security plan,'" and "counsel[s] against many of the specific practices" alleged in the complaint.[26] The court also pointed to the FTC's published complaints and consent decrees in administrative cases raising unfairness claims based on inadequate corporate cybersecurity,[27] noting that "all of the allegations in at least one of the relevant four or five complaints have close [factual] corollaries here."[28]

Implications of the *Wyndham* Decision

- **The FTC and state regulators will cite the opinion to bolster their claims to cybersecurity jurisdiction.** The FTC will undoubtedly cite the opinion to support its claim to authority to regulate cybersecurity as litigation arises in other circuits, and may use the opinion as a justification to pursue even more such cases. In addition, the many state Attorneys General who enforce statutes modeled on the FTC Act--so called "Little FTC Acts"--will attempt to use the opinion and the Third Circuit's reasoning to bolster their jurisdictional claims.

- **Data security practices that resonate with a non-technical audience play an outsized role in cybersecurity litigation.** The Third Circuit panel noted that Wyndham allegedly "failed to use *any* firewall at critical network points, did not restrict specific IP addresses *at all*, did not use *any* encryption for certain customer files, and did not require some users to change their default or factory-setting passwords *at all*," highlighting the potential significance in litigation of cybersecurity risks that can be succinctly summarized for a non-technical audience.[29]

- **Regulators' published guidance provides a starting point for companies assessing their cybersecurity preparedness.** The court's reference to published FTC guidance underscores the value of consulting guidance from the FTC and other government agencies when developing cybersecurity policies and practices.

- **Privacy policies and other public-facing disclosures may be cited in cybersecurity litigation.** According to the court, "[a] company does not act equitably when it publishes a privacy policy to attract customers who are concerned about data privacy, [and then] fails to make good on that promise by investing inadequate resources in cybersecurity."[30] Periodic

re-examination of privacy policies and other public-facing documents can help companies avoid this issue.

- **Even companies that have not suffered a data breach may find themselves in regulators' crosshairs.** While *Wyndham* involved a target that allegedly experienced multiple breaches, the FTC does not regard its authority as being limited to such circumstances, and there is nothing in the court's decision that explicitly limits the agency's regulatory jurisdiction to instances in which a company has suffered a data breach or customers have suffered an actual loss.

---

[1] *See F.T.C. v. Wyndham Worldwide Corp.*, No. 14-3514, 2015 WL 4998121 (3d Cir. Aug. 24, 2015) ("*Wyndham*").

[2] *See* FTC, Press Release, "Third Circuit rules in FTC v. Wyndham case" (Aug. 25, 2015), *available at* https://www.ftc.gov/news-events/blogs/business-blog/2015/08/third-circuit-rules-ftc-v-wyndham-case?utm_source=govdelivery.

[3] 15 U.S.C. § 45(a)(1).

[4] *See Wyndham*, 2015 WL 4998121, at *3–5.

[5] *See* FTC, "Commission Statement Marking the FTC's 50th Data Security Settlement" (Jan. 31, 2014).

[6] *Id.*

[7] *In the Matter of LabMD*, Dkt. No. 9357 (Complaint filed Aug 29, 2013), *available at* https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter. Like Wyndham, LabMD challenged the Commission's authority to regulate data security practices. Pursuant to the FTC's administrative litigation procedures, the Commission ruled on, and denied, that motion. *See id.* (Order Denying Motion to Dismiss (Jan. 16, 2014)). LabMD also challenged the FTC's right to pursue litigation in the Eleventh Circuit and by seeking a preliminary injunction in the Northern District of Georgia. Those efforts were unsuccessful. *See LabMD, Inc. v. FTC*, No. 13-15267, 2014 U.S. App. LEXIS 9802 (11th Cir. Feb. 18, 2014); *LabMD, Inc. v. FTC*, 776 F.3d 1275 (11th Cir. 2015). If the FTC rules on the merits that LabMD's data security practices violated Section 5, LabMD has the right to appeal to a federal circuit court of its choosing that otherwise possesses jurisdiction. *See* FTC, Guide to Antitrust Laws, The Enforcers, *available at* https://www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws/enforcers.

[8] FTC, "Commission Statement Marking the FTC's 50th Data Security Settlement" (Jan. 31, 2014).

[9] Complaint ¶ 47, *FTC v. Wyndham Worldwide Corp.*, 2012 WL 12146600 (D.N.J. June 26, 2012) (No. 13CV01887) (amended Aug. 9, 2012).

[10] *Id.* at ¶ 24.

[11] *Wyndham*, 2015 WL 4998121, at *3; *see FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D.N.J. 2014) ("*Wyndham Worldwide*").

[12] *Wyndham Worldwide*, 10 F. Supp. 3d at 631–632; *Wyndham*, 2015 WL 4998121, at *3.

[13] *Wyndham*, 2015 WL 4998121, at *1.

[14] *Id.* at *5 (citing 15 U.S.C. § 14(n)).

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] *Id.* at *6.

[20] *Id.* (citing 15 U.S.C. § 45(n)).

[21] *Id.* (emphasis in original).

[22] *Id.* at *7–8.

[23] *Id.* at *8–9.

[24] *Id.* at *13.

[25] *Id.* at *14 (internal citations omitted; emphasis in original).

[26] *Id.* at *14.

[27] Although the complaints and consent decrees are not "adjudications on the merits," the court found them to be persuasive evidence that the FTC believes an alleged practice fails the cost-benefit analysis articulated in § 45(n), because FTC commissioners must vote on whether to issue a complaint. *Wyndham*, 2015 WL 4998121, at *15.

[28] *Id.* The court acknowledged that "it may be unfair to expect private parties back in 2008 to have examined FTC complaints or consent decrees." *Id.* at *15, n.23. But, Wyndham did not argue that it was unaware of the consent decrees or complaints. *Id.*

[29] *Id.* at *14 (emphasis in original).

[30] *Id.* at *5.

The following Gibson Dunn lawyers prepared this client alert: M. Sean Royall, Alexander H. Southwell, Ryan T. Bergsieker, Richard H. Cunningham, Danielle Serbin, and Jordan C. Jacobsen.

Gibson, Dunn & Crutcher's lawyers are available to assist with any questions you may have regarding these issues and have substantial experience counseling companies on data security issues, developing data breach response plans, responding to data breaches, navigating FTC investigations, and litigating against both private plaintiffs and government enforcers. For further information, please contact the Gibson Dunn lawyer with whom you usually work or any of the following members of the firm's Privacy, Cybersecurity and Consumer Protection Group:

United States

M. Sean Royall - Co-Chair, Dallas (+1 214-698-3256, sroyall@gibsondunn.com)
Alexander H. Southwell - Co-Chair, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
Debra Wong Yang - Co-Chair, Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)
Howard S. Hogan - Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)
Karl G. Nelson - Dallas (+1 214-698-3203, knelson@gibsondunn.com)
Joshua A. Jessen - Orange County and Palo Alto (+1 949-451-4114/+1 650-849-5375, jjessen@gibsondunn.com)
Michael Li-Ming Wong - San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com)
Ryan T. Bergsieker - Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
Richard H. Cunningham - Denver (+1 303-298-5752, rhcunningham@gibsondunn.com)
Eric D. Vandevelde - Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)

Europe

James A. Cox - London (+44 207 071 4250, jacox@gibsondunn.com)
Andrés Font Galarza - Brussels (+32 2 554 7230, afontgalarza@gibsondunn.com)
Kai Gesing - Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Bernard Grinspan - Paris (+33 1 56 43 13 00, bgrinspan@gibsondunn.com)
Alejandro Guerrero Perez - Brussels (+32 2 554 7218, aguerreroperez@gibsondunn.com)
Jean-Philippe Robé - Paris (+33 1 56 43 13 00, jrobe@gibsondunn.com)
Michael Walther - Munich (+49 89 189 33-180, mwalther@gibsondunn.com)

China
Kelly Austin - *Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)*

India
Jai S. Pathak - *Singapore (+65 6507 3683, jpathak@gibsondunn.com)*